Global Data and Cyber Handbook - New Zealand

Key Data & Cybersecurity Laws

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# How are data and cybersecurity laws/regulations implemented?

*Last review date: 20 December 2024*

☒  omnibus – all personal data

☒  sector-specific — e.g., financial institutions, governmental bodies

Health, telecommunications, civil defense, credit reporting, justice sector (unique identifiers), and superannuation schemes (as currently provided for in codes of practice)

Data privacy and security are also addressed in a range of other sector-specific laws, such as the Health Act 1956.

# What are the key data privacy laws and regulations?

*Last review date: 20 December 2024*

The key legislation governing privacy in New Zealand is the Privacy Act 2020 (**Privacy Act**). The Privacy Act sets out 13 Information Privacy Principles (each an **IPP**) that govern (among others) the collection, storage and security, accuracy, retention, use and disclosure of personal information.

The Privacy Commissioner may also issue a code of practice under the Privacy Act in relation to particular industries and sectors (each a **Privacy Code**). A Privacy Code may modify the application of any of the IPPs as they apply with respect to specified information or classes of information, specified agencies or classes of agencies, an industry or profession, or a class of industries or professions.

# What are the key cybersecurity laws and regulations?

*Last review date: 20 December 2024*

New Zealand does not have specific cybersecurity laws and regulations.

The Privacy Act addresses cybersecurity through the application of IPP 5. IPP 5 requires an agency to ensure that personal information it holds is protected by such security safeguards as it is reasonable in the circumstances to take, against:

Loss

Access, use, modification, or disclosure that is not authorized by the agency and other misuse

# What are the key laws and regulations relating to non-personal data?

*Last review date: 20 December 2024*

New Zealand does not have specific laws or regulations relating to non-personal data.

# Are new or material changes to those key data and cybersecurity laws anticipated in the near future?

*Last review date: 20 December 2024*

Yes.

In November 2024, the Privacy Commissioner recommended a specific set of amendments to modernize the Privacy Act in line with technological advancements. The proposed amendments focus on the following topics:

introducing a right for individuals to request that their data be erased

establishing a stronger penalty regime for breaches of the Privacy Act

requiring agencies to demonstrate how they meet their privacy requirements, such as the privacy management programs recommended by the OECD, and

introducing stronger protections for automated decision making like artificial intelligence

On 18 December 2024, the Privacy Commissioner announced plans to issue a Biometrics Processing Privacy Code of Practice (**Code**). A draft code, along with proposed guidance, has been released for public consultation. Previously, an exposure draft of a biometrics processing privacy code was released, which received significant public feedback. The current consultation focuses on an amended version of that exposure draft.

Alongside the Code, the Office of the Privacy Commissioner (OPC) has released draft guidance to explain the application of the rules, how the Code is intended to work, and how organizations can comply with it. The draft guidance currently covers guidance on rules 1, 2, 3, 6, and 10, which generally address the purpose of collection, individuals’ rights of access, and limits on the use of biometric information. These rules are considered to significantly impact the application of the Privacy Act.

The Code addresses the key privacy risks identified by the Commissioner in relation to biometric information and includes three key proposals:

A **proportionality assessment** would require agencies to carefully consider whether their reasons for using biometrics outweigh the privacy intrusion or risks.

**Transparency and notification requirements** would place greater obligations on agencies to be open and transparent with individuals and the public about their collection and use of biometric information.

**Purpose limitations** would put some restrictions on collecting and using biometric information for certain reasons.

The Privacy Amendment Bill, which was first released in 2023, has now reached its second reading in Parliament. Once passed, it will make changes to the current personal information notification regime under the Privacy Act 2020. The Privacy Amendment Bill proposes to broaden the notification requirements under IPP 3, so that it will apply when agencies collect information about an individual indirectly. Currently, there is no requirement for an agency to notify an individual when it collects personal information indirectly.

The Bill will introduce a new IPP 3A that will apply to indirect collection and will closely mirror the requirements and exceptions of IPP 3. Agencies will not need to comply with the new IPP 3A if they reasonably believe that:

the relevant information is publicly available information

compliance would prejudice either the security or defense of New Zealand or the international relations of the Government

compliance would reveal a trade secret, or

compliance would cause a serious threat to public health or safety, or the health or safety of another individual.

IPP 3A will not apply to personal information collected before 1 June 2025.

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.